THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of generating a key over a group of order q, said method including the steps of:

   generating a seed value from a random number generator;

   performing a hash function on said seed number to provide an output;

   determining whether said output is less than said prime number q;

   accepting said output for use as a key if the value thereof is less than said prime number q; and

   rejecting said output as a key if said value is not less than said order q.

2. The method of claim 1 wherein another seed value is generated by said random number generator if said output is rejected.

3. The method of claim 1 wherein the step of accepting said output as a key includes a further step of storing said key.

4. The method of claim 1 wherein said key is used for generation of a public key.

5. The method of claim 1 wherein said order q is prime number represented by a bit string of predetermined length l.

6. The method of claim 5 wherein said output from said hash function is a bit string of predetermined length l.

7. The method of claim 1 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

8. The method of claim 7, wherein said step of incrementing includes a further step of adding a particular value to said seed value.

9. A method of generating a key over a group of order q, said method including the steps of:

   generating a seed value from a random number generator;

   performing a hash function on said seed number to provide a first output;

incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output;

combining said first output and second output to produce a new output;

determining whether said new output has a value less than said order q;

accepting said new output as a key k if said new output has a value less than order q; and rejecting said new output as a key if said new output has a value less than order q

10. The method of claim 9 wherein upon rejection of said new output a new seed value is generated by said random number generator.

11. The method of claim 9 wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained.

12. The method of claim 9 wherein a bit string greater than a predetermined length l is obtained and an l bit string selected therefrom for comparison with said order q.

13. The method of claim 12 wherein upon rejection of said bit string of predetermined length l, a further l bit string is selected.

14. The method of claim 9 wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l.